# UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

477 West Main Street, Room 47B, Waukesha, WI 53186, a rooming house in a three story brick building, more fully described in Attachment A.

Case No 20-853M(NJ)

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, Sections 875(d) and 2256(8)(a).

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Christina Porter
*Applicant's signature*

FBI Task Force Officer Christina Porter
*Printed Name and Title*

Sworn to before me and signed in my presence:

Date: January 15, 2020

*Judge's signature*

City and State: Milwaukee, Wisconsin

Hon. Nancy Joseph, U.S. Magistrate Judge
*Printed Name and Title*

# AFFIDAVIT

I, Christina Porter, being first duly sworn, hereby depose and state as follows:

1. I am a detective with the West Allis Police Department and am currently assigned to the Sensitive Crimes Unit. I have been a law enforcement officer since May of 2004. As part of my official duties, I am assigned as a task force officer (TFO) to the Federal Bureau of Investigation's (FBI) Child Exploitation Task Force, Milwaukee Division. As part of my duties as a detective and TFO, I investigate violations of law relating to child pornography and exploitation. I have gained experience in conducting these investigations through training and through my everyday work as a Sensitive Crimes Detective and a TFO. That work frequently includes executing search warrants and conducting interviews of subjects suspected of trading and manufacturing of child pornography or otherwise sexually exploiting children with the use of technology. I have received training relating to the investigation of Internet Crimes Against Children (ICAC), including training in the investigation and enforcement of state and federal child pornography laws in which computers and other digital media are used as a means for receiving, transmitting, and storing child pornography.

2. The facts contained in this affidavit are known to me through my personal knowledge, training, and experience, as well as through information provided to me by other law enforcement officers whom I consider to be truthful and reliable. Some of the information was provided in response to administrative subpoenas and search warrants. I believe this information is reliable because it was provided by independent companies in response to court or agency requests.

3. Based upon the information described below, I submit there is probable cause to believe that within 477 W. Main St., Room 47B, Waukesha, WI, as further described in Attachment A, and here within referred to as "subject premises," there are records, files, correspondence, memoranda, computers, tablets, cellular phones and other electronic devices, electronic storage media, bank and other financial records, data, and other materials that constitute evidence of, the fruits of, or instrumentalities of criminal violations including extortion, 18 U.S.C. Section 875(d), and the distribution of child pornography, 18 U.S.C. Section 2256(8)(a).

4. Because this affidavit is being submitted for the limited purpose of establishing probable cause for the requested warrant, it does not set forth all of my knowledge about this matter. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits and instrumentalities of the violations of the federal statutes named above are located within the subject premises. The information contained in this affidavit came from my own participation in the investigation, as well as from other law enforcement officers, and information gained from my personal training and experience.

## DEFINITIONS

5. The following definitions apply to the affidavit and Attachment B to this affidavit:

a. "Camera" means a device used for recording visual images in the form of photographs, film, or video signals. Digital cameras record and store images in

a digital format, which can include Digital8, MiniDV, DVD, a hard drive, or solid-state flash memory.

b. "Cellular telephone" or "cell phone" means a hand held wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geolocation information indicating where the cell phone was at particular times.

c. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but are not, in and of themselves, legally obscene or do not necessarily depict minors in sexually explicit conduct.

d. "Child Pornography" is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is

indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

e. "Cloud" or "cloud storage" is a mechanism in which files can be saved to an off-site storage system maintained by a third party – i.e., files are saved to a remote database instated of the (user's) computer's hard drive. The internet provides the connection between the user's computer and the database for saving and retrieving files.

f. "Computer" is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

g. "Computer Server" or "Server," is a computer attached to a dedicated network and serves many users. A web server, for example, is a computer that hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system (DNS) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (IP) address so the computer hosting the web site may be located, and the DNS server provides this function.

h. "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

i. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

j. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

k. "Computer passwords, pass phrases and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass phrase (a string of alphanumeric characters) usually operates as a sort of digital key to "unlock" particular data security

devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys that perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

l. "Electronic storage devices" includes computers, cellular telephones, tablets, and devices designed specifically to store electronic information (e.g., external hard drives and USB "thumb drives"). Many of these devices also permit users to communicate electronic information through the Internet or through the cellular telephone network (e.g., computers, cellular telephones, and tablet devices such as an iPad).

m. "Hash Value" refers to the process of using a mathematical function, often called an algorithm, to generate a numerical identifier for data. A hash value can be thought of as a "digital fingerprint" for data. If the data is changed, even slightly, (like the addition or deletion of a comma or a period), the hash value changes. Therefore, if a file such as a digital photo is a hash value match to a known file, it means the digital photo is an exact copy of the known file.

n. "Internet Service Providers" (ISPs) are commercial organizations in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications

equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

o. "An Internet Protocol address" (IP address) is a unique numeric address used by internet-enabled electronic storage devices to access the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every electronic storage device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to the electronic storage device may be directed properly from its source to its destination. Most ISPs control a range of IP addresses. Some computers have static – that is, long-term – IP addresses, while other computers have dynamic – that is, frequently changed – IP addresses.

p. "Media Access Control" (MAC) address means a hardware identification number that uniquely identifies each device on a network. The equipment connecting a computer to a network is commonly referred to as a network

adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter. This MAC address is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

q. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

r. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including writings and drawings), photographic form (including prints, negatives, videotapes, motion pictures, and photocopies), mechanical form (including printing and typing) or electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

s. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or

masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

t. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use URLs on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

u. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

ELECTRONIC STORAGE DEVICES AND FORENSIC ANALYSIS

6. I have consulted with laypersons and law enforcement officers with specialized knowledge and training in computers, networks, and Internet communications. In particular, I consulted with FBI SA Neil Lee, who has received specialized training as a forensic computer, cellular telephone, and other electronic storage device examiner. SA Lee has been a forensic computer examiner with the FBI since 2015. SA Lee has participated in the execution of numerous search warrants and search and seizure operations. SA Lee has informed me to properly retrieve and analyze electronically stored (computer) data, and to insure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the electronic storage

devices. To affect such accuracy and completeness, it may also be necessary to analyze not only the electronic storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the device computer and software. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the proposed search location, in whatever form they are found. One form in which the records might be found is stored on a computer's hard drive, other storage media, or within a hand-held electronic device such as a cellular telephone or a tablet device (e.g., an iPad device). Some of this electronic information, as explained below, might take a meaningful form only upon forensic analysis.

7. Based on my knowledge, training, and experience, and after having consulted with SA Lee, I know computer and other electronic device hardware, peripheral devices, software, electronic files, and passwords may be important to a criminal investigation in three distinct and important respects:

a. The objects themselves may be instrumentalities used to commit the crime;

b. The objects may have been used to collect and store information about crimes (in the form of electronic data);

c. The objects may be contraband or fruits of the crime.

8. I submit that if a computer or other electronic storage device is found on the premises, there is probable cause to believe information will be saved to that electronic storage device, for the following reasons:

a. Based on my knowledge, training, and experience, I know electronic storage device files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person deletes a file on an electronic storage device, the data contained in the file does not actually disappear; rather, the data remains on the storage medium until it is overwritten by new data. Deleted files, or remnants of deleted files, may reside in free space or slack space, that is, in space on the storage medium that is not currently being used by an active file for long periods before they are overwritten. In addition, if the electronic storage device uses an operating system (in the case, for example, of a computer, cellular telephone or tablet device) the device may also contain a record of deleted data in a swap or recovery file.

b. Wholly apart from user-generated files, electronic storage device storage media, in particular, computers' internal hard drives, contain electronic evidence of how the device was used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, and file system data structures. Electronic storage device users typically do not erase or delete this evidence, because special

software is typically required for that task. However, it is technically possible to delete this information.

c. Files viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or cache. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

9. As further described in Attachment B, this application seeks permission to locate not only electronic storage device files that might serve as direct evidence of the crimes described on the warrant, but also for evidence establishing how electronic storage devices were used, the purpose of their use, who used them, and when.

10. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), electronic storage device storage media can contain other forms of electronic evidence as described below:

a. Data on the storage medium not currently associated with any file can provide evidence of a file once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage

devices or other external storage media, and the times the electronic storage device was in use. Electronic storage device file systems can record information about the dates files were created and the sequence in which they were created.

b. As explained herein, information stored within an electronic storage device and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within an electronic storage device (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the electronic storage device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the electronic storage device was remotely accessed, thus inculpating or exculpating the electronic storage device owner. Further, electronic storage device activity can indicate how and when the electronic storage device was accessed or used. For example, as described herein, computers typically contain information that logs computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to

understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within an electronic storage device may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer or cellular telephone may show a particular location and have geolocation information incorporated into its file data. Such file data typically contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera). The geographic and timeline information described herein may either inculpate or exculpate the electronic storage device user. Last, information stored within an electronic storage device may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information within the electronic storage device may indicate the owner's motive and intent to commit a crime (e.g., Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the electronic storage device or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on an electronic storage device is relevant to the investigation may depend on other information stored on the electronic storage device and the application of knowledge

about how an electronic storage device works. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

d. Further, in finding evidence of how an electronic storage device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, I know from training and experience it is possible malicious software can be installed on a computer, often without the computer user's knowledge, which can allow the computer to be used by others, sometimes without the knowledge of the computer owner.

11. I know from my training and experience, as well as from information found in publicly available materials, that some electronic devices offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") which is read via an integrated biometric device in lieu of a numeric or alphanumeric passcode or password. This feature often referred to as a fingerprint scanner, a fingerprint reader, or for Apple devices, Touch ID.

12. If a user enables the fingerprint scanner on a given device, he or she can register multiple fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's fingerprint scanner, which can be found in different locations on the device depending on the manufacturer. In my training and experience, users of devices that offer fingerprint scanners often enable it because it is considered a more

convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

13. In some circumstances, a fingerprint cannot be used to unlock a device that has its fingerprint scanner enabled, and a passcode or password must be used instead. Thus, in the event law enforcement encounters a locked device, the opportunity to unlock the device via the fingerprint scanner exists only for a short time. The fingerprint scanner also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) too many unsuccessful attempts to unlock the device via the fingerprint scanner are made.

14. If fingerprint scanner enabled devices are found during a search of the premises, the passcode or password that would unlock such devices are presently unknown to law enforcement. Thus, it will likely be necessary to press the fingers of the user(s) of any device(s) found during the search of the premises to the device's fingerprint scanner in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the device(s) via fingerprint scanner with the use of the fingerprints of the user(s) is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

15. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via the fingerprint scanner, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Further, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the premises to press their finger(s) against the fingerprint scanner of the locked device(s) found during the search of the premises in order to attempt to identify the device's user(s) and unlock the device(s) via the fingerprint scanner.

16. Based upon my knowledge, training and experience, and after having consulted with SA Lee, I know a thorough search for information stored in storage media often requires agents to seize most or all storage media to be searched later in a controlled environment. This is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media in a controlled environment, it is often necessary that some electronic storage device equipment, peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:

a. The nature of evidence. As noted above, not all evidence takes the form of documents and files easily viewed on site. Analyzing evidence of how an electronic storage device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable.

b. The volume of evidence. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. Technical requirements. Electronic storage devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of electronic storage device hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

17. In light of these concerns, I hereby request permission to seize the electronic storage devices, associated storage media, and associated peripherals believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude it would be impractical to search the hardware, media, or peripherals on-site for this evidence.

18. I know when an individual uses a computer to commit crimes involving child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic storage device is an instrumentality of the crime because it is used as a means of committing the criminal offense. From my training and experience, I believe an electronic storage device used to commit a crime of this type may contain evidence of how the electronic storage device was used, data sent or received, notes as to how the criminal conduct was achieved, records of Internet discussions about the crime, and other records that indicate the nature of the offense.

## CASE BACKGROUND

19. On June 20, 2016, I conducted a federal investigation under case number 305A-MW-8882841/17-CR-04 whereby Xavier T. Douglas was indicted. In that investigation, Xavier Douglas, while posing as a juvenile female online, obtained nude

images from an identified juvenile male with the initials of CH (full information is known by law enforcement). Xavier, while posing as a girl, threatened to expose CH's nude images unless he sent more. CH ended up locating his nude images on Twitter and other public websites. CH's mother then filed a police report. Simultaneously, the FBI also received a Cybertip from the National Center for Missing and Exploited Children which reported that a Twitter account in the name of "clayexposed," later determined to have been created by Xavier Douglas, contained nude images of CH.

20. On June 30, 2016, a search warrant was executed at Xavier Douglas' residence at the time, and the contents of his electronic devices was analyzed. Nude and clothed images of CH were located, in addition to chats regarding another juvenile named GMP (full information is known by law enforcement - GMP is now an adult).

21. During his interview, Xavier Douglas admitted to creating fake accounts online and he would post anything he had to in order to make the accounts popular. Then he would promote himself on those accounts, so his account with his true identity would become popular. Xavier admitted to creating fake Facebook accounts in various names, including the name of CH and GMP. He said when he came across CH and GMP' real social media accounts and he saw how popular they were, Xavier decided to create fake accounts in those names while using pictures of CH and GMP from their real accounts. Xavier also admitted that after obtaining the nude images of CH, he posted on the fake CH social media accounts that he has been exposed, which made his accounts even more popular. Xavier said once he had a lot of attention, he would be

able to promote his own, real social media accounts and his goal was to get paid by social media for using their applications.

22. Xavier was also asked during his interview what extortion is and Xavier said using information against someone to get what you want or blackmail. Special Agent Brett Banner told Xavier he was using sextortion with CH since he was telling CH to send more stuff or it's going to be leaked on the internet. Xavier understood this and was aware it was illegal. It was also explained to Xavier that he was producing child pornography since CH was under 18 years of age at the time.

23. Xavier was federally indicted for the production of child pornography, interstate extortion threat, and distribution of child pornography. He ultimately pleaded guilty to stalking by use of a computer system on May 1, 2017. He was sentenced to 16 months in the Federal Bureau of Prisons, followed by three years of supervised release (which Xavier is still under).

## DETAILS OF THE INVESTIGATION

24. On September 25, 2019, I was contacted by Special Agent (SA) Laura Goshen from the FBI in Baltimore, Maryland. She informed me that she had been contacted by Detective Trevor Teague of the St. Mary's County Sheriff's Office (Maryland) who was investigating a case that appeared to involve Xavier T. Douglas, m/b, XX/XX/94 extorting victim JS (full name is known by law enforcement) with threats of exposing photographs purchased by JS that Xavier claimed to be of child pornography. SA Goshen checked the FBI database and located the previous case

(305A-MW-8882841) I had investigated involving Xavier. SA Goshen inquired if I could get into contact with Det. Teague to assist with his investigation.

25. On September 26, 2019, I spoke with Det. Teague and he briefed me on his current investigation. I noticed some similarities in his investigation to my past investigation involving Xavier Douglas. Since I was aware that Xavier was residing in the area of Waukesha, WI, and that the victim in the case lived in Maryland, I offered to take the investigation over federally. Det. Teague agreed to this and forwarded me all of the information he had obtained through the course of his investigation thus far.

26. Upon reviewing the reports from the St. Mary's County Sheriff's Office and the information received through the issuance of subpoenas and search warrants, I determined that victim JS had agreed to purchase links, which included images of pornography, from an individual, believed to be Xavier Douglas, on the online chatting application called Snapchat in November of 2018. The name on the Snapchat account from which the links were purchased by JS was "GMP." Per JS, "GMP" was selling nude images of himself on Snapchat. JS informed me that he observed "GMP" advertising that he was selling "nudes" on his Snapchat story, which JS assumed would be adult pornography. I am aware that Snapchat is a multimedia messaging application that allows pictures and messages to usually be only available for a short period of time before they become inaccessible to their recipients.

27. JS paid for the links by use of PayPal, which is a worldwide online payments system that supports online money transfers and serves as an electronic alternative to traditional paper methods like checks and money orders. The company

operates as a payment processor for online vendors, auction sites, and other commercial users, for which it charges a fee in exchange for benefits such as one-click transactions and password memory. JS sent the money to the PayPal account in the name of paypal.me/XAYPREME. JS was told by "GMP" to send the money to Xavier Douglas at this account. Once the payment was made, JS received a link to Dropbox, and JS downloaded the images from the link onto his cellular phone. JS believed some of the images he received were of "GMP" because his pictures matched the Snapchat profile picture for GMP. There was one nude image of "GMP," and after the purchase was complete, the Snapchat profile in the name of GMP re-contacted JS and informed him that GMP was actually 17 years of age and that JS had just purchased child pornography.

28. The individual operating the GMP Snapchat account told JS that JS would have to send him additional money through the PayPal account or else "GMP" would report JS to the FBI for purchasing child pornography. JS did not know if the image was child pornography and he complied with the demands and began sending more money to the PayPal account in the name of paypal.me/XAYPREME. JS reported that several other people were also possibly involved in the extortion scheme since he began to get contacted by various other individuals on Snapchat, Instagram and via text message to JS' cell phone. The phone number used to text JS was 262-997-8355. Per Det. Teague, this phone number was determined to belong to US Cellular, and on October 7, 2019 a subpoena has been issued to US Cellular for the number's subscriber information. On November 7, 2019, Det. Teague forwarded the results of this subpoena

to me, which showed that this phone account belongs to Xavier Douglas of 477 W. Main St., Waukesha, WI.

29. JS then began receiving Snapchat messages from a party with the Snapchat username with the initials of "CH." This full name is known by law enforcement and is the same name used in the previous investigation involving Xavier. This individual told JS to start sending the money to a different PayPal account with the name of paypal.me/Xavierluxemburg. JS sent money to the two PayPal accounts 21 times, and he was sometimes sending the value of his entire paycheck to prevent this party from reporting him to the FBI for purchasing child pornography. JS also told me that he began to get contacted by unknown individuals who were offering to help give JS money since he was in college and was giving all his money to Xavier Douglas. These individuals were using the Instagram screen names of matthewmellonjr, alyxmogilevich, themicahfaulkner, and richgenofig. These individuals told JS to keep giving Xavier money and they would later forward money back to JS to help him out. JS never received any money from these people and I believe Xavier Douglas was likely operating these accounts in order to get JS to send him more money. I asked JS if he had any further account information for these individuals and he did not because he deleted his social media accounts after making the initial police report and he said these individuals kept using different account names. I was unable to locate the social media accounts operated by these alleged individuals.

30. Det. Teague completed and served a search warrant to PayPal to obtain records pertaining to the PayPal accounts in the names of paypal.me/XAYPREME and

paypal.me/Xavierluxemburg. The search warrant results showed that both of these accounts had been created by Xavier Douglas with a date of birth of XX/XX/94, an address of 477 W. Main St., Waukesha, WI 53186 and email addresses of Xaviertluxemburg@gmail.com and xavierklatten@gmail.com. Det. Teague also informed me that there were multiple other individuals who had made payments to these two PayPal accounts, some of who had made multiple payments and may also be extortion victims.

31. On October 1, 2019 I received an email from Xavier Douglas' federal probation agent, Agent Andrew Cieslewicz. I discussed this investigation with Agent Cieslewicz and he advised that about one month earlier, Xavier had told Agent Cieslewicz that he needed rent money and he asked Agent Cieslewicz for assistance with this. Agent Cieslewicz also confirmed that Xavier resided at 477 W. Main St., Waukesha, WI with the phone number of 414-865-0528. Agent Cieslewicz advised that this address is a rooming house and Xavier tends to move between rooms in the building as they become available. I also noticed that the phone number for Xavier of 414-865-0528 was the phone number used to create both of the PayPal accounts in question.

32. On October 1, 2019 I reviewed all of the Paypal search warrant records for the accounts belonging to Xavier Douglas, which had the associated Paypal account numbers of 1851961769800210616 and 1744137058497529456. For account with ID number 1851961769800210616, the transactions were provided between the dates of

November 1, 2018 and August 20, 2019. Under the Payments Received section of the spreadsheet, I located the following payments made to the account from JS:

11/25/18 $100.00

11/25/18 $100.00

11/25/18 $150.00

11/26/18 $200.00

03/07/19 $500.00

03/21/19 $405.00

For the account with ID number 1744137058497529456, the transactions were provided between the dates of November 1, 2018 and August 20, 2019. Under the Payments Received section of the spreadsheet, I located the following payments made to the account from JS:

04/18/19 $5.00

04/18/19 $500.00 (denied)

04/18/19 $500.00 (denied)

04/18/19 $500.00 (denied)

04/18/19 $499.00

05/02/19 $625.00 (denied)

05/02/19 $625.00 (denied)

05/02/19 $613.84

05/16/19 $574.00

05/30/19 $579.69

06/13/19 $627.00

06/27/19 $590.00

07/11/19 $667.70

07/25/19 $588.95

08/08/19 $590.65

The total amount of money sent from JS to Xavier was $7,208.83.

33. According to the initial report from the St. Mary's Sheriff's Department, JS had provided screen shots from his cell phone of information pertaining to this case. On September 30, 2019, I requested a copy of these screen shots from Det. Teague. On October 1, 2019, these images were emailed to me. I reviewed the screen shots. Two of the screen shots were lists of some of the money JS sent to Xavier Douglas. In one of the screen shots, the profile picture was of the real Xavier Douglas, who I recognized from my previous investigation with him. Another screen shot had a message from Xavier Douglas which stated:

> "GMP said if you dont contact him on Snapchat he is going to contact your school with all the information he has about you and your child pornography."
>
> Another screen shot said:
>
> "I told him last week that IDC if he sends you money. Hell his money could help you pay me off but I guess he's worried bout some bad publicity or some shit. Either way IDC. See you in 2 weeks. Try your best for 600."

Lastly, another screen shot stated:

"TBH I was gonna come back at you on the 31st for another $700. But TBH I'll only need $200 on the 31st then we are all good and if anyone comes at you after that you send

them my wayb."

34. On October 2, 2019 I was contacted by Agent Cieslewicz who advised he had some of Xavier's bank account information which may be helpful to my investigation. I reviewed the information provided by Agent Cieslewicz. There was a screen shot of Xavier's Venmo application, which showed the screen name as Xavier Douglas and the username as @XWAIMZ. There was also a screen shot of banking information which only showed Xavier's name, the email address of thexaviertdouglas@gmail.com, the phone number of 661-262-9384, the address of 477 W. Main St., #11, Waukesha, WI, the routing number of 031101279, and the account number of 156118204999. This routing and account number is the same routing and account number provided in the PayPal search warrant return for Xavier's PayPal account with the account number 1851961769800210616. This routing and account number are listed as being Xavier's checking account information through The Bancorp Bank.

35. Agent Cieslewicz also forwarded a screen shot of Xavier's personal Snapchat account, which has the display name of Xavier and username of xavierdecaux. It should be noted that two of the email addresses associated with the one of the PayPal accounts were similar names of XavierTDecaux@gmail.com and xecaux@gmail.com. A

screen shot was also provided which showed a list of some of Xavier's friends on Snapchat and one of the names was the display name with the initials of CH with a username of hain32. On October 30, 2019, I requested an administrative subpoena be issued to Snapchat for the subscriber information used to register the account with the username of hain32. I received those results on November 18, 2019, which showed that the email address associated with this account is xxxxxxxx@gmail.com and the IP address used to create the account was 65.30.129.50 on May 25, 2016 at 21:14 UTC. I then determined that this IP address was assigned to Charter Communications by using the WhoIs Arin IP Address Lookup Database website. An administrative subpoena was then issued to Charter Communications to determine what customer account was assigned this IP address on May 25, 2016 at 21:14 UTC. Charter Communications responded back that they do not have these records anymore.

36. On October 23, 2019 I submitted an administrative subpoena to Google requesting the subscriber information on the various email accounts which were associated with the two PayPal accounts in Xavier's name. The email addresses listed on the PayPal search warrant results that are associated with the PayPal accounts are Xavierluxemburg@gmail.com, xavierklatten@gmail.com, XavierTDecaux@gmail.com and xecaux@gmail.com. On November 7, 2019, I received the subpoena results. Two IP addresses used to access the email account xavierklatten@gmail.com were 65.30.143.233 and 24.209.131.183. I used the Arin WhoIs IP Address Database website to determine that these IP addresses are assigned to Charter Communications. An administrative subpoena was submitted to Charter Communications to see who the subscriber was

who was assigned these two IP addresses at times when the email address xavierklatten@gmail.com was utilized. The results showed that both IP addresses were assigned to Jennifer Dowling of 477 W. Main St., Room 35, Waukesha, which is the same rooming house where Xavier is residing.

37. I submitted a surveillance request so surveillance could be conducted on Xavier at his residence at 477 W. Main St. in Waukesha. On October 21, 2019, I was informed that Xavier was being assigned to a new probation agent by the name of Agent Patricia Savasta. Agent Savasta confirmed that Xavier was still residing at this rooming house and was currently living in room 47B. She also confirmed his employment at Wal-Mart, located at 2000 S. West Avenue in Waukesha. On November 5, 2019 and November 6, 2019, surveillance was conducted at 477 W. Main St., Waukesha, but Xavier was not observed. On November 21, 2019, Agent Savasta met with Xavier in person and confirmed that he was currently residing in Room 47B and he had no plans to move. Per Agent Savasta, Xavier said he quit his job at Wal-Mart and was now working as the rooming house manager, so he does not go out much.

38. On October 29, 2019 I spoke with JS and inquired about the images he had purchased from the party he met on Snapchat using the name of "GMP." Det. Teague had tried to recover these images from JS' cell phone, but was unable to since JS had deleted them after he was told they may contain child pornography. JS told me that he had made three initial purchases, which was one purchase per link, so he purchased a total of three Dropbox links. Each link contained images of a different male. The first link JS believed contained images of who JS believed was GMP. There was one nude

full-body image of GMP and a few clothed, selfie-type images of GMP. JS told me that he conducted a Google Images internet search of the name GMP and found multiple results, including the clothed images from the link. JS said it appeared that these were images for GMP' social media accounts. JS took screen shots on his cell phone of the images he located of GMP online which were the same images from the link he purchased and forwarded those pictures to me. The second file JS purchased was about eight or nine images of the same unknown male, and one video of the male. This male is nude, but JS said he could not tell if the male was a juvenile or adult. The third file JS purchased was four or five nude images of another unknown male. He also could not determine if this male was an adult or child.

39. On October 29, 2019, I conducted an internet search on Google for "GMP." There were multiple results stating that he is a popular Instagram star from Texas. Several pictures of him appear online, and the images of GMP match the person in the pictures that were forwarded to me from JS. Per the website, birthdaycelebs.com/GMP/, GMP was born in Texas on XX/XX/2000, making him 18 years old. It states that GMP is a "social media personality best known for his engaged following on Instagram and Twitter. He has also dabbled in YouTube, Vine and YouNow." Based on GMP being a known person on social media and YouTube, the fact that Xavier Douglas has used his name as a fake persona in a previous investigation, that the images of GMP could make a person believe he was a juvenile, and that none of the accounts used to extort JS belonged to GMP or registered to an IP address in Texas

where GMP is believed to reside, I felt that Xavier Douglas was posing on SnapChat as GMP and was using public images of GMP from the internet.

## CHARACTERISTICS COMMON TO INDIVIDUALS WHO RECEIVE AND POSSESS CHILD PORNOGRAPHY

40. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who receive and possess images of child pornography:

a. Individuals who receive and possess child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals who receive and possess child pornography may collect sexually explicit or suggestive materials, in a variety of media, including electronically, or through photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who receive and possess child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.

d. Individuals who receive and possess child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

e. Individuals who receive and possess child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

## BACKGROUND ON ELECTRONIC STORAGE DEVICES AND CHILD PORNOGRAPHY

41. Computers, cellular telephones, and other electronic storage devices (collectively electronic storage devices) have dramatically changed the way in which individuals interested in child pornography interact with each other. Electronic storage

devices basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

42. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a device by simply connecting the camera to the electronic storage device. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards can store terabytes of data, which provides enough space to store thousands of high-resolution photographs. Video recorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the video recorder to a computer. Many electronic storage devices (e.g., computers, cellular telephones, and tablets), have cameras built into the device which allows users to create and store still and video images on the device. Moreover, if the device has Internet connectivity, users can distribute still and video images from the device.

43. Internet-enabled electronic storage devices can connect to other Internet-enabled devices. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child

pornography can be transferred via e-mail or through file transfer protocols (FTPs) to anyone with access to an Internet-enabled electronic storage device. Because of the proliferation of commercial services that provide e-mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, electronic storage devices are the preferred method of distribution and receipt of child pornographic materials.

44. Electronic storage devices are the ideal repository for child pornography. The amount of information an electronic storage device can hold has grown exponentially over the last decade. Electronic storage devices can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on a computer or other electronic storage device. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Many electronic storage devices can easily be concealed and carried on an individual's person.

45. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

46. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and

Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any internet-enabled electronic storage device. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's electronic storage device in most cases.

47. As is the case with most digital technology, communications by way of electronic storage device can be saved or stored on the device. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, an electronic storage device user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

48. Based on my knowledge, training, and experience, I know electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a device, the data

contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, I believe the images described by JS from the links he purchased are still located in and can be retrieved from the electronic storage devices at the Subject Premises.

FINANCIAL RECORDS

49. Based on my knowledge and experience and information gathered from this investigation, I know that individuals involved in extortion schemes tend to maintain records, in either paper or electronic format or a combination of the two, regarding contacts with potential victims, details surrounding the money received, receipts, bank records, payment records and other financial transaction information, and other information which can be used to memorialize payments received. I am aware that when individuals attempt to extort multiple victims at once, they tend to maintain some type of documentation in regards to their potential victims.

50. I am aware that individuals involved in extortion schemes frequently retain records of their transactions within places under their control, such as their homes. These records may be in the form of written notes and correspondence, receipts, negotiated instruments, contacts, bank statements, other records and may consist of electronic or paper records.

51. I am also aware that individuals use electronic equipment, such as computers, tablets, Personal Data Assistants (PDAs), disk drives, USB drives, CD-ROMS, DVD-ROMS, memory chips, cellular phones, digital cameras, scanners and/or facsimile machines to generate and store, transfer or print documents containing

information regarding their financial transactions. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of crime, contraband, instrumentalities of crime, and/or fruits of crime. In this case, I believe any computer, cell phone, or other electronic device used by Xavier Douglas may be a container for evidence because computers often maintain data directly on their hard drives and therefore remain potentially recoverable. I know that Xavier Douglas used an electronic device which can connect to the internet to communicate with the victim(s) in this case.

52. As previously discussed in regards to the possession of child pornography, I am aware that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the internet. Even when such files have been deleted, they can be recovered months or years later using readily-available forensic tools.

## CONCLUSION

53. I submit this affidavit supports probable cause for a warrant to search the premises described in Attachment A and seize the items described in Attachment B.

ATTACHMENT A

Description of Subject Property

The subject property, 477 West Main Street, Room 47B, Waukesha, WI 53186, is a rooming house in a three story brick building. The windows on the front of the building, which faces West Main Street, have white trim and the first floor windows are covered with a white awning which have the words "Wisconsin House" printed on them. There are cement steps leading to the main front door, which is a common entrance into the building. The main front door is brown in color. The numbers "477" are affixed to the front of the building in white lettering. The premises includes any storage areas or units within the building at 477 West Main Street, Waukesha, WI that is assigned to Room 47B. The premises also includes all containers that may contain magnetic, optical, or digital media within the real property, located at 477 West Main Street., Room 47B, Waukesha, WI.


Golden
Moments
Gottlieman

ATTACHMENT B

Property to Be Seized

All evidence, instrumentalities, information, records, and contraband relating to violations of Title 18, United States Code, Sections 2252A(a)(2) (distribution of child pornography, including:

1. Records and information concerning the of occupancy of the Premises;

2. Cellular telephones, telephone and address books, and other notes and papers insofar as they memorialize, include, or confirm computer screen names, contact information, or images related to the Offense;

3. Records in any form or other items or materials that pertain to Internet service, as well as records relating to the ownership or use of computer equipment found in the residence;

4. Computers or storage media used to commit the Offense, which will be identified during a subsequent search of the seized and imaged computers and storage media;

5. Records containing child pornography or pertaining to the distribution, receipt or possession of child pornography;

6. Routers, modems, and network equipment used to connect computers to the Internet;

7. With respect to any computer equipment or other electronic devices (hereinafter "computer") used to facilitate or commit the Offense:

   a. evidence of who used, owned, or controlled the computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

   b. evidence of software that would allow others to control the computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the computer of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer;

h. evidence of the times the computer was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the computer;

j. documentation and manuals that may be necessary to access the computer or to conduct a forensic examination of the computer;

k. records of or information about Internet Protocol addresses used by the computer;

l. records of or information about the computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

8. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

9. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

10. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

In addition to all evidence, instrumentalities, information, records, and contraband relating to violations of Title 18, United States Code, Section 875(d) (extortion) including:

11. Any and all financial records related to any and all banking or credit accounts, to include but not limited to: bank statements, checks, loan records, credit card records, ledgers, check registers, credit cards, lines of credit, deposit records, wire transfer detail, and money transfer records.